

ELIOT SPITZER  
Attorney General

STATE OF NEW YORK  
OFFICE OF THE ATTORNEY GENERAL  
120 BROADWAY, NEW YORK, NEW YORK 10271

DIVISION OF PUBLIC ADVOCACY

SUSANNA M. ZWERLING  
Bureau Chief  
Bureau of Telecommunications and Energy  
E-mail: Susanna.Zwerling@OAG.State.NY.US  
Vox: (212) 416-8083  
Fax: (212) 416-8877

November 8, 2004

Ms. Marlene H. Dortch  
Office of the Secretary  
Federal Communications Commission  
445 12<sup>th</sup> Street S.W. Suite TW-A325  
Washington, D.C. 20554

Re: In the Matter of Communications Assistance for Law Enforcement Act and  
Broadband Access and Services, ET Docket No. 04-295

Dear Ms. Dortch:

Pursuant to the Commission's Notice of Proposed Rulemaking adopted August 4, 2004 in the above referenced proceeding, please find enclosed the Comments of New York State Attorney General Eliot Spitzer. Enclosed with this letter are the original executed brief and affidavit of John Christopher Prather (Exhibit A) which were e-filed in unsigned form.

Sincerely,

Susanna M. Zwerling  
Assistant Attorney General in Charge  
Telecommunications and Energy Bureau

Enclosure: Comments of NYS Attorney General and Exhibits

cc: Natek, Inc.  
9300 East Hampton Drive  
Capitol Heights, MD 20743

Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, D.C. 20554

In the Matter of  
Communications Assistance for Law Enforcement  
Act and Broadband Access and Services

)  
)  
)  
)  
)  
)

ET Docket No. 04-295  
RM-10865

**Comments of Eliot Spitzer  
Attorney General of the State of New York**

Susanna M. Zwerling  
Assistant Attorney General in Charge  
Telecommunications and Energy Bureau  
*of counsel*

John Christopher Prather  
Deputy Attorney General  
Organized Crime Task Force

New York State Attorney General's Office  
120 Broadway  
New York, NY 10271  
(212) 416-6343, Fax (212) 416-8877  
Susanna.Zwerling@oag.state.ny.us

November 8, 2004

## **TABLE OF CONTENTS**

SUMMARY .....	1
BACKGROUND .....	1
INTEREST OF THE ATTORNEY GENERAL OF THE STATE OF NEW YORK .....	4
ARGUMENT .....	5
I.    The Commission Should Apply CALEA to Broadband Technologies .....	5
A.    Applicability of CALEA Need Not Turn on a Service's Classification as an Information Service or Telecommunications Service Under the 1996 Act ..	5
B.    Services Which Substantially Replace Existing Telephone Service are Subject to CALEA .	7
1. Subject VoIP and other broadband services to CALEA .....	8
2. Subject multimedia wireless messaging services to CALEA .....	10
II.    The FCC Should Adopt And Enforce Deadlines For Compliance. ....	11
III.   The FCC Should Regulate Which Costs Carriers May Impose On Law Enforcement. ....	12
CONCLUSION .....	16
Exhibit A:	
AFFIDAVIT OF J. CHRISTOPHER PRATHER sworn to November 8, 2004	

## SUMMARY

The Office of New York State Attorney General Eliot Spitzer (“NY OAG”) hereby submits these comments pursuant to the Federal Communications Commission’s (“FCC” or “Commission”) *Notice of Proposed Rulemaking In the Matter of Communications Assistance for Law Enforcement Act and Broadband Access and Services* (“NPRM”)<sup>1</sup>. In the NPRM, the FCC tentatively concluded that most packet-mode or Internet protocol (“IP”) services are subject to the provisions of the Communications Assistance to Law Enforcement Act (“CALEA”).<sup>2</sup> The NY OAG supports that tentative conclusion, and offers comments on the FCC’s proposals in order to establish rules implementing that conclusion. By establishing deadlines for carriers’ compliance with CALEA and ensuring that the costs imposed upon law enforcement agencies (“LEAs”) do not inhibit the agencies’ ability to effect court-authorized intercepts, the FCC can effectuate the intent of Congress in adopting CALEA: ensuring law enforcement’s continued ability to implement court-authorized interceptions in the face of changing communications technologies.

## BACKGROUND

In adopting CALEA in 1994, Congress recognized that certain technological advances were inhibiting law enforcement’s ability to effect lawful intercepts of communications of terrorists, members of organized crime, and other criminal targets. The statute was intended:

to preserve the government’s ability, pursuant to court order or other lawful authorization, to intercept communications involving advanced techniques such as digital or wireless transmission modes, or features and services such as call forwarding, speed dialing and conference calling, while protecting the privacy of

---

<sup>1</sup> *Notice of Proposed Rule Making, In the Matter of Communications Assistance for Law Enforcement Act and Broadband Access and Services*, ET Docket No. 04-295.

<sup>2</sup> Public Law 103-414, 108 Stat. 4279 (1994), 47 U.S.C. § 1001.

communications and without impeding the introduction of new technologies, features, and services.<sup>3</sup>

Court-authorized intercepts of telephone communications have been, and continue to be, an essential investigative tool used by State and Federal law enforcement. New York State law enforcement, especially the NY OAG's Statewide Organized Crime Task Force ("OCTF") uses such intercepts to solve major crimes and obtain convictions of organized crime leaders and members of international drug cartels.<sup>4</sup> As the number of telecommunications services employing packet-mode or IP technology has increased exponentially, the number of services not technically accessible to court-authorized intercepts pursuant to a valid warrant has also increased.<sup>5</sup>

In recent years a tremendous amount of business traffic has migrated to the internet and the number of residential users who are choosing to replace their phone service with Voice over Internet Protocol (VoIP) telephony continues to grow each month.<sup>6</sup> Additionally, most wireless carriers now offer phones with features such as multimedia messaging services which rely upon packet-mode or IP technologies. Undoubtably, among those increasingly using packet-mode and IP based services

---

<sup>3</sup> *CALEA Legislative History*, *supra* at 3489.

<sup>4</sup> Exhibit A, Affidavit of John Christopher Prather, sworn to November 8, 2004 ("Prather Aff.") ¶ 11.

<sup>5</sup> *See also* New York Criminal Procedure Law Article 700; Prather Aff. ¶ 5.

<sup>6</sup> *See e.g.*, Cablevision Press Release, September 13, 2004, "With more than 115,000 customers as of June 30, Optimum Voice is the fastest-growing and most widely-deployed digital voice-over-cable service in the nation;" *See also*, Vonage Press Release, October 29, 2004 "With More than 300,000 lines in service, Vonage continues to add more than 25,000 lines per month...;" *See also Barrons*, May 24, 2004, *Talk Gets Cheap*, at 19-22 (22 million households now have broadband access, making broadband-based VoIP services like Vonage a threat to wireline carriers; Net2Phone has 100,000 U.S. customers; prepaid calling cards using VoIP were used by an estimated 1.2 million people in 2003 and are expected to reach 1.3 million in 2004; Cox is beginning to offer IP telephony to its million circuit-switched customers; Comcast, with 1.2 million circuit-switched subscribers is preparing to launch an IP telephony service).

will be criminals and terrorists.<sup>7</sup> Unless the FCC moves quickly pursuant to this NPRM to clarify that all of these services are subject to the requirements of CALEA, an increasing portion of communications traffic will be unavailable to law enforcement despite the issuance of a court order.

The FCC has both the authority and duty under CALEA to ensure compliance by all providers. Compliance can only be effected through the establishment of enforceable deadlines. The NY OAG disagrees with the Commission's statement that "Law Enforcement's goal can be achieved without us imposing the implementation deadlines it requests,"<sup>8</sup> and seeks the establishment of explicit and brief time periods for carriers to come into compliance with CALEA.

Finally, too many carriers appear to be treating CALEA as a profit center by imposing unreasonably high fees to effect intercepts. The NY OAG strongly supports the Commission's tentative conclusion that "carriers bear responsibility for CALEA development and implementation costs for post-January 1, 1995 equipment and facilities"<sup>9</sup> and seeks specific rules outlining those costs which carriers may or may not recover from LEAs.

---

<sup>7</sup> Experience shows that criminals, particularly sophisticated ones, quickly find and exploit these holes, especially when, in the case of VoIP telephony there is little change in the means of communication. *See* Affidavit of J. Christopher Prather, Deputy Attorney General, Statewide Organized Crime Task Force, sworn to November 8, 2004 at ¶ 14-15 ("Prather Aff."), and attached as Exhibit A.

<sup>8</sup> *NPRM* at ¶ 91.

<sup>9</sup> *Id.* at ¶ 125.

**INTEREST OF THE ATTORNEY GENERAL OF THE STATE OF NEW YORK**

The NY OAG is the chief law enforcement officer for the State of New York. As such, the NY OAG falls within the definition of “government” as set forth in CALEA.<sup>10</sup> A core mission of the NY OAG is investigating sophisticated criminal enterprises, cases that often rely on court-authorized intercepts. A major bureau within the NY OAG’s criminal division is the Statewide Organized Crime Task Force which investigates and prosecutes multi-county, multi-state, and multi-national organized criminal activities occurring within New York State.<sup>11</sup> New York long has been a key center for the investigation, interruption, and prosecution of narcotics trafficking and other major organized crime activities. The NY OAG’s facilities, particularly OCTF’s wiretap plants, routinely are used to assist other state, local, and federal law enforcement agencies.<sup>12</sup> These efforts account for roughly 30% of all wiretaps conducted nationally.<sup>13</sup>

---

<sup>10</sup> See 47 U.S.C. § 1001(5).

<sup>11</sup> See N.Y. Exec. Law § 70-a. OCTF works closely with local, state and federal law enforcement agencies to investigate and prosecute organized criminal activities such as loan sharking, gambling rings, narcotic trafficking, racketeering, and money laundering. OCTF’s investigations of traditional organized crime are too numerous to catalogue, however, the most notable have included electronic surveillance of associates of the Colombo and Gambino crime families. Prather Aff. ¶9. OCTF is a leading partner in narcotics task forces throughout New York, providing legal, investigative and technical expertise. Sheriff’s offices, district attorneys, and municipal police officers from different counties participate in these task forces. *Id.* ¶3. A cooperative effort between the State Police and OCTF on the Cali Cartel Project, which ran from 1986 to 2003, is undoubtedly the paragon of interagency partnerships in New York State, having resulted in the arrest of nearly 450 major narcotics traffickers and the seizure of more than eleven tons of cocaine and over \$60 million in cash. In addition to OCTF, the NY OAG’s Criminal Prosecutions Bureau is responsible for the investigation and prosecutions of criminal actions within the jurisdiction of the Attorney General. The NY OAG’s Medicaid Fraud Control Unit investigates and prosecutes health care crime in New York State. The NY OAG’s Public Integrity Unit handles complex investigations into government corruption, fraud and abuse of authority. Among other statutes, the Public Integrity Unit enforces the “Tweed Law.” N.Y. Exec. Law § 63-c. As New York State’s chief legal officer, the NY OAG represents the New York State Police and other state agencies.

<sup>12</sup> Exhibit A, Prather Aff. ¶ 3.

<sup>13</sup> *Id.*

Further, the NY OAG represents New York State's interest in numerous federal and state court trials and regulatory proceedings, including many FCC dockets.

## ARGUMENT

### I. The Commission Should Apply CALEA To Broadband Technologies.

The NY OAG agrees with the Commission's tentative conclusion that "facilities-based providers of any type of broadband Internet access, including but not limited to wireline, cable modem, satellite, wireless, and broadband access via the powerline...are subject to CALEA."<sup>14</sup>

While the Commission bases this tentative conclusion solely on the provision of the CALEA statute that requires that services that "provide replacement for a substantial portion of the local telephone exchange service,"<sup>15</sup> the NY OAG believes that that conclusion should rest as well on the applicability of CALEA to services that are provided by telecommunications carriers that are not information services for the purposes of CALEA.<sup>16</sup> A determination based upon both of these statutory provisions will ensure LEAs the ability to access all services that fall into the ambit of CALEA.

#### A. Applicability of CALEA Need Not Turn on a Service's Classification as an Information Service or Telecommunications Service Under the 1996 Act.

As the Commission points out in the NPRM, Congress made CALEA applicable to "telecommunications carriers" but excluded from this group "persons or entities insofar as they are

---

<sup>14</sup> *NPRM* at ¶ 47

<sup>15</sup> *Id.*

<sup>16</sup> 47 U.S.C. § 1001(8)(C)(i).



engaged in providing information services.”<sup>17</sup> Because providers of packet-mode or IP based wireline or wireless services are “telecommunications carriers” for the purposes of CALEA and those services are not “information services” as contemplated by that statute, they are required to comply with CALEA.

In separate dockets, the Commission has been considering whether cable modem services,<sup>18</sup> wireline-based broadband services<sup>19</sup> and VoIP<sup>20</sup> are “telecommunications services” or “information services” for the purposes of the 1996 Telecommunications Act (“1996 Act”).<sup>21</sup> While those determinations will have, among other things, profound impacts on carriers’ costs, and are thus subject of much contention, the distinction contemplated by the 1996 Act is inapposite here.<sup>22</sup>

CALEA provides that “telecommunications carriers” are relieved of their CALEA obligations only “insofar as they are engaged in providing information services.”<sup>23</sup> Therefore, while

---

<sup>17</sup> *NPRM* at ¶ 50 citing 47 U.S.C. § 1001(8)(C)(i).

<sup>18</sup> *Declaratory Ruling and Notice of Proposed Rulemaking*, In the Matter of Inquiry Concerning High-Speed Access to the Internet over Cable and Other Facilities, 17 FCC Rcd 3019 (2002), *reversed in part and remanded*, *Brand X v. FCC*, 345 F.3d 1120 (9<sup>th</sup> Cir. 2003), *rehearing en banc denied* \_\_ F. 3<sup>rd</sup> \_\_, (9<sup>th</sup> Cir. April 1, 2004).

<sup>19</sup> *Notice of Proposed Rule Making*, In the Matter of Appropriate Framework for Broadband Access to the Internet Over Wireline Facilities, et al., CC Docket 02-33 17 FCC Rcd 3019 (2002).

<sup>20</sup> *See, Notice of Proposed Rule Making*, In the Matter of IP-Enabled Services, FCC 04-28, WC Docket 04-36 (Adopted: February 12, 2004). *See also, Memorandum Opinion and Order*, In the Matter of Petition for Declaratory Ruling that pulver.com’s Free World Dialup is neither Telecommunications Nor a Telecommunications Service, Memorandum Opinion and Order, WC 03-45, (Adopted: Feb. 12, 2004).

<sup>21</sup> 47 U.S.C. § 251, *et seq.*

<sup>22</sup> In Comments filed before this Commission in response to the *Notice of Proposed Rule Making* In the Matter of IP-Enabled Services, WC Docket No. 04-36, May 28, 2004, the NY OAG argued that “Because some VoIP services are beginning to substitute for traditional ... telephone services, a host of regulatory policies that apply to common carriers are implicated by the move to VoIP services” at 2.

<sup>23</sup> 47 U.S.C. § 1001(8)(C)(i).

the 1996 Act's use of the terms "telecommunications service" and "information service" are mutually exclusive, this is not so with CALEA. Though in the *NPRM* the Commission distances itself from the language of the 1999 *Second Report and Order* In the Matter of Communications Assistance for Law Enforcement Act,<sup>24</sup> that *Order* nonetheless recognizes that the CALEA definitions are not mutually exclusive, stating that where "facilities are used to provide both telecommunications and information services . . . such joint-use facilities are subject to CALEA."<sup>25</sup> Thus, the Commission "conclude[d] as a matter of law that the entities and services subject to CALEA must be based on the CALEA definition . . . independently of their classification for the separate purposes of the Communications Act."<sup>26</sup> It is therefore entirely proper to find that a service is not an "information service" for the purposes of CALEA even if the Commission determines that it is an "information service" under the 1996 Act.

B. Services Which Substantially Replace Existing Telephone Service are Subject to CALEA

As the Commission pointed out in the *NPRM*, the definition of a "telecommunications carrier" in CALEA is broader than the definition of "telecommunications carrier" in the 1996 Act.<sup>27</sup> For CALEA purposes, a "telecommunications carrier" includes both an entity engaged in "the transmission or switching of wire or electronic communications as a common carrier for hire"<sup>28</sup> and

---

<sup>24</sup> *NPRM* at footnote 131.

<sup>25</sup> *Second Report and Order* In the Matter of Communications Assistance for Law Enforcement Act, CC Docket No. 97-213, 15 FCC Rcd 7105 (1999) at ¶ 27.

<sup>26</sup> *Id* at ¶ 13.

<sup>27</sup> *NPRM* at ¶ 52.

<sup>28</sup> 47 U.S.C. § 1001(8)(A). As the Commission recognizes in the *NPRM*, CALEA's inclusion of the term "switching" is not limited to only circuit-mode switching but instead CALEA's general use of "switching" should be interpreted to include packet-mode switching as well. *NPRM* at ¶ 48.

an entity providing transmission service “to the extent that the Commission finds that such service is a replacement for a substantial portion of the local telephone exchange service and that it is in the public interest to deem such person or entity to be a telecommunications carrier for purposes of this subchapter.”<sup>29</sup>

As described earlier, more and more business service is being routed over the Internet, thousands of residential customers are switching to VoIP services, and wireless providers are offering services over packet-mode and IP-based technologies.<sup>30</sup> The providers of these services are certainly “telecommunications carriers” in that their services include transmission or switching and replace a “substantial portion” of the local telephone service as contemplated by CALEA. Requiring carriers to make these services accessible to law enforcement as Congress directed in CALEA is clearly in the public interest.

1. Subject VoIP and other broadband services to CALEA.

The NY OAG supports the Commission’s tentative conclusion that CALEA applies to broadband technologies, including most of those that employ VoIP and other packet-mode technologies.<sup>31</sup> The NY OAG, however, does not agree with the Commission’s conclusion that what it refers to as “non-Managed” VoIP services, those services that are disintermediated and in which “the VoIP provider has minimal or no involvement in the flow of packets during communication”<sup>32</sup> should be exempt from CALEA.

---

<sup>29</sup> *Id.* at § 1001(8)(B)(ii).

<sup>30</sup> *See NPRM* at ¶ 7.

<sup>31</sup> *Id.* at ¶ 37.

<sup>32</sup> *Id.*

In adopting CALEA, Congress clearly intended that communications transmitted over the Internet are subject to CALEA.<sup>33</sup> While Congress in 1994 could not have anticipated the specific Internet-based communications applications, let alone the multiple variations on VoIP, that have emerged, this sort of technology change is precisely the type of development that Congress intended to be addressed by CALEA. Where a target's phone calls have been subjected to court-authorized interception, the target's choice of an "Internet phone" service in place of a circuit-switched phone service should not determine whether law enforcement can or cannot monitor the call.

As the NY OAG has recently experienced, criminals, like other consumers, are switching their services to residential VoIP. Earlier this year, in investigating narcotics-related crimes, the NY OCTF executed a court-ordered wiretap on a phone in Central New York. Right after the wiretap was implemented, the target, keeping the same phone number, switched to VoIP service provided by Time Warner Cable. Time Warner Cable cooperated with the New York State police in putting the wiretap into effect on its VOIP system. As a result of this wiretap, the OCTF succeeded in seizing four kilos of cocaine, an extraordinary amount for Central New York, and arrested eight individuals.<sup>34</sup>

The NY OAG disagrees with the Commission's tentative conclusion that non-managed VoIP services should not be subject to the requirements of CALEA. In this era of heightened security

---

<sup>33</sup> *CALEA Legislative History, supra* at 3503-04. ("While the bill does not require reengineering of the Internet, nor does it impose prospectively functional requirements on the Internet, this does not mean that communications carried over the Internet are immune from interception or that the Internet offers a safe haven for illegal activity. Communications carried over the Internet are subject to interception under Title III [of the Crime Control Act] just like other electronic communications. That issue was settled in 1986 with the Electronic Communications Privacy Act.")

<sup>34</sup> Prather Aff. ¶ 16.

concerns, it is not only in the public interest to ensure that all providers of telecommunications services *including non-managed VoIP services* are subject to CALEA, it would be dangerous to exempt these services from law enforcement's access.

To the extent that the Commission bases its tentative conclusion on the argument that non-managed VoIP services are private networks, the NY OAG respectfully disagrees as these services are available to all subscribers with broadband access, including, those engaged in criminal activity. A determination that these services are exempt from CALEA would create a "tap free zone" for use in communications by criminals and terrorists.

As VoIP services of all kinds replace public switched telephone services, the public interest is not only consistent with making VoIP services subject to CALEA, but *demand*s the Commission make such determination immediately, before even greater migration of telephony onto VoIP networks limits law enforcement to intercepting only those calls that remain on the circuit-mode switched network.

2. Subject wireless multimedia messaging services to CALEA.

Wireless telecommunications that include packet-mode or IP based multimedia messaging services should be declared subject to CALEA because they provide both telecommunications and information services. CALEA's use of both "wire or electronic communications" in the foregoing definitions goes beyond traditional voice telephony, and explicitly includes "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by wire, radio, electromagnetic, photoelectronic or photooptical system."<sup>35</sup> Thus, wireless technologies

---

<sup>35</sup> Section § 1001(1) of CALEA incorporates the definition of "electronic communication" in 18 U.S.C. § 2510(12).

that provide video messaging and picture messaging are subject to CALEA, regardless of how they might be classified for the very different purposes of the 1996 Act.

## II. The FCC Should Adopt and Enforce Deadlines For Compliance.

The NY OAG supports the FCC's proposal that all carriers must come into compliance with any determinations on *existing* extension petitions within 90 days and the concurrent proposal that the Commission restrict the availability of future compliance extensions to carriers, particularly those using packet-mode technologies. The NY OAG, however, disagrees with the Commission's conclusion that "Law Enforcement's goal can be achieved without us imposing the implementation deadlines" requested by Law Enforcement.<sup>36</sup> Only if the Commission establishes deadlines for carriers' compliance with CALEA will any determination that packet-mode and IP based services are subject to CALEA be effectuated.

In order to effect the goal not only of law enforcement but of Congress in adopting CALEA, the Commission should establish an aggressive time period for carriers' compliance with CALEA. Exceptions to these deadlines should be rare rather than, as they are currently, automatically granted for a period of two years. Given the lack of economic incentive for carriers to bring their technologies into compliance with CALEA, not to mention the track record of extensions on top of extensions, the NY OAG is not optimistic about the carriers' timely compliance with CALEA in the absence of enforceable deadlines, which we urge the Commission to impose and enforce.

---

<sup>36</sup> NPRM at ¶ 91.

Deadlines are only as good as the enforcement mechanism behind them. The Commission therefore should clarify the rules by which CALEA compliance deadlines are to be enforced. The mere fact that Congress also allowed aggrieved parties and the Commission the power to seek the intervention of the Courts do not limit the Commission's enforcement capabilities.<sup>37</sup> In light of the critical mission of law enforcement and the carriers' track record of delays in deploying technology needed to assist law enforcement with court-authorized intercepts, effective application of CALEA to new technologies requires the establishment of deadlines and the implementation of a process for enforcing them.

### III. The FCC Should Regulate Which Costs Carriers May Impose On Law Enforcement.

In the NPRM, the Commission tentatively concluded that "carriers bear responsibility for CALEA development and implementation costs."<sup>38</sup> The NY OAG agrees with that conclusion, and urges the FCC to implement specific rules effecting the intent of Congress that while law enforcement may be required to compensate carriers for provisioning expenses associated with a particular wiretap, the costs of CALEA compliance are to be borne by the carriers.

In CALEA, Congress established a compensation scheme to ensure implementation of the statute. For equipment deployed before January 1, 1995, Congress appropriated \$500 million "to pay telecommunications carriers for all reasonable costs directly associated with the modifications

---

<sup>37</sup> See 47 U.S.C. §1007.

<sup>38</sup> NPRM at ¶125.

performed ... to establish the capabilities necessary to comply with [CALEA].”<sup>39</sup> For facilities and equipment deployed after 1995, the statute places the cost of implementing CALEA compliance on the carrier, except where the Commission makes a determination that compliance is not “reasonably achievable” because it “would impose significant difficulty or expense on the carrier or on the users of the service.”<sup>40</sup> Only where the Commission finds that compliance is not reasonably achievable without subsidization would that carrier have a basis to apply for funds; in fact, no such findings have ever been issued and carriers therefore are responsible for the costs of post-1995 compliance.

The costs of individual interceptions are addressed in the Crime Control Act, which authorizes carrier compensation for the costs incident to each wiretap order. Under the Act, “any provider of wire or electronic communication service ... shall be compensated therefor by the applicant for reasonable expenses incurred in providing such facilities or assistance.”<sup>41</sup> This statute allows carriers to collect the cost of provisioning an individual interception from the LEA making the interception request, but limits the amount that the LEA may be charged to the reasonable expenses incurred in responding to the individual wiretap warrants, as opposed to the costs of achieving capability as prescribed by CALEA.

---

<sup>39</sup> 47 U.S.C. § 1008(a).

<sup>40</sup> *Id.* at § 1008(b)(1). Congress listed eleven factors in making such determinations of reasonable achievability, the first of which is “the effect on public safety and national security.” The other factors to be considered include, *inter alia*, the effect on rates for basic residential telephone service, protection of privacy for communications not authorized to be intercepted, the policy to encourage provision of new technologies and services, carriers’ financial resources, and competition impacts. Congress intended that “industry will bear the cost of ensuring that new equipment and services meet the legislated requirements.” See *CALEA Legislative History*, *supra* at 3496..

<sup>41</sup> 18 U.S.C. § 2518(4)(emphasis added).



The explicit language of CALEA and the Crime Control Act and the practical effect of including compliance costs in the amount charged to LEAs both make clear that these costs were never intended to be passed along to law enforcement. For example, in 1999, the Commission anticipated that the wireless carriers would pay approximately \$159 million and the wireline carriers would pay approximately \$117 million to implement CALEA compliance with four of the FBI “punch-list” items.<sup>42</sup> Based upon these estimates, recovery of all carriers’ CALEA compliance capital costs through individual wiretap provisioning fees, given the close to 1,500 annual court authorized intercepts, could result in charges as great as \$10,000 to \$50,000 per intercept.<sup>43</sup> Obviously, this cost recovery scheme would make intercepts prohibitively expensive for virtually all law enforcement agencies, and would result in depriving law enforcement of an essential crime fighting and anti-terror tool. There is no basis for concluding that Congress intended this result.

Despite the statutory language and the practical effect of charging law enforcement for the costs of compliance, it is nonetheless our experience that many carriers are charging the NY OAG and other law enforcement agencies far more than their “reasonable expenses incurred in providing facilities and assistance” to effect authorized intercepts.

As fully set forth in the attached Affidavit of J. Christopher Prather, the fees many carriers charge the NY OAG are neither reasonable nor related to expenses incurred in provisioning a wiretap.<sup>44</sup> For example, wireless carriers charge from \$1,500 to \$4,400 to set up an intercept, plus

---

<sup>42</sup> *Third Report and Order*, In the Matter of Communications Assistance for Law Enforcement Act, CC Docket No. 97-213, 14 FCC Rcd. 16,794, (1999) Appendix B at n.2.

<sup>43</sup> “*Report of the Director of the Administrative Office of the United States Courts, on Applications for Orders Authorizing or Approving the Interception of Wire, Oral or Electronic Communications*,” (2003) at Table 2.

<sup>44</sup> See Exhibit A ¶¶ 16-22.

between \$250 and \$2,200 monthly to maintain it. The reasonable wireless carrier expenses incurred to execute a warrant should not be significantly more than the same carriers' normal fees to provide basic wireless services to business customers (ranging from \$135 to \$400 monthly),<sup>45</sup> and probably much less (since the intercept is effected with a few keystrokes at a computer terminal).<sup>46</sup> Intercept provisioning fees cost the NY OAG between \$400,000 and \$500,000 annually.<sup>47</sup> As burdensome as this expense is for New York State, other smaller-scale law enforcement agencies simply cannot afford to pay the fees many carriers are demanding, and instead must forego using wiretaps entirely.<sup>48</sup>

As the above examples demonstrate, the fees many carriers' charge to the NY OAG for provisioning intercepts exceed the carriers' reasonable expenses incurred in providing the intercept as permitted by 18 U.S.C. § 2518(4). It appears that some carriers are attempting to collect from law enforcement the capital and other costs of meeting CALEA implementation capacity requirements and not just the incremental expenses of provisioning individual intercepts. The Commission,

---

<sup>45</sup> For example, AT&T Wireless charges \$299 per month for 3000 local/long distance minutes to small business customers. <http://www.attwireless.com/business/plans/overview.jhtml>. At Sprint PCS, a similar small business plan with 2,500 minutes (plus unlimited minutes to other PCS phones or during off-peak hours) costs \$135 per month. [http://www.sprint.com/pcsbusiness/plans/voice/free\\_clear.html](http://www.sprint.com/pcsbusiness/plans/voice/free_clear.html). Nextel charges \$100 for 2,000 minutes (plus unlimited off-peak usage). Cingular charges \$250 for 4,500 monthly anytime minutes (plus 5,000 off-peak minutes). Verizon Wireless offers 3,500 monthly minutes (plus unlimited off-peak minutes) for \$200. <http://www.verizonwireless.com/b2c/store/controller?item=planFirst&action=viewPlanDetail&sortOption=priceSort&catId=323>. T-Mobile's 4,000 minutes per month (plus unlimited off-peak and mobile-to-mobile minutes) costs \$200.

<sup>46</sup> Exhibit A, Prather Aff., ¶¶ 17-19. In general, wireline carriers (including ILECs and CLECs) charge the NY OAG much less for installing an intercept than do wireless carriers.

<sup>47</sup> *Id.* ¶ 17.

<sup>48</sup> *Id.* ¶ 18.

therefore, should exercise its authority under § 229(a) of the 1996 Act<sup>49</sup> and promulgate regulations that define those costs carriers may properly recover from law enforcement through provisioning fees, consistent with the directives in CALEA and the Crime Control Act.

### CONCLUSION

Because of the critical role that court-authorized intercepts play in both State and Federal law enforcement, law enforcement agencies must have the ability to intercept all telecommunications services as contemplated by CALEA. As more and more telecommunications services employ packet-mode or IP technology, it is crucial that the FCC clarify that these services are subject to the requirements of CALEA, set deadlines for carriers' compliance, and define those provisioning costs that may be charged to law enforcement. The nation's security depends upon its law enforcement agencies' access to these services.

November 8, 2004

Respectfully submitted,

ELIOT SPITZER  
Attorney General of the State of New York

By:

---

Susanna M. Zwerling  
Assistant Attorney General in Charge  
Telecommunications and Energy Bureau

---

<sup>49</sup> 47 U.S.C. § 229(a).

For Public Inspection

New York State Attorney General's Comments  
November 8, 2004

Susanna M. Zwerling  
Assistant Attorney General in Charge  
Telecommunications and Energy Bureau  
*of counsel*

John Christopher Prather  
Deputy Attorney General  
Organized Crime Task Force

New York State Attorney General's Office  
120 Broadway  
New York, NY 10271  
(212) 416-6343  
Fax (212) 416-8877  
Susanna.Zwerling@oag.state.ny.us

**Exhibit A**

Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, D.C. 20554

In the Matter of	)	
	)	RM-10865
United States Department of Justice, Federal Bureau	)	
of Investigation, and Drug Enforcement Agency	)	AFFIDAVIT OF
	)	J. CHRISTOPHER
	)	PRATHER
Joint Petition for Rulemaking to Resolve Various	)	
Outstanding Issues Concerning the Implementation of the	)	
Communications Assistance for Law Enforcement Act.	)	

STATE OF NEW YORK     )  
  ) ss.:  
COUNTY OF NEW YORK    )

J. Christopher Prather, being duly sworn, deposes and says:

1.       I am an employee of the Office of the Attorney General of the State of New York ("OAG"), jointly appointed by New York's Attorney General and the Governor of New York to the position of Deputy Attorney General in Charge of the Statewide Organized Crime Task Force

("OCTF"). I have held this position since September 2002.<sup>50</sup> I am fully familiar with the facts stated herein.

### The Organized Crime Task Force

2. OCTF was established in 1970 by the enactment of Section 70-a of the New York Executive Law. OCTF has broad powers to investigate organized criminal activity occurring in more than one county in New York State or occurring both within and outside of New York State.

3. OCTF has offices across the State of New York and conducts long-term investigations into narcotics trafficking, gambling, money laundering, smuggling, labor racketeering, prostitution, grand larceny, official corruption, and fraud. OCTF provides assistance, as requested and whenever possible, to local district attorneys' offices, especially technical assistance with wiretaps. OCTF also provides assistance and intelligence to various federal law enforcement agencies with whom it works, including the United States Federal Bureau of Investigation ("FBI"), Drug Enforcement Agency, Secret Service, Department of Labor-Inspector General, Bureau of Alcohol, Tobacco and Firearms, and the U.S. Attorneys' offices. More than one-third of all court-approved wiretaps in the nation are done in New York.

4. The Deputy Attorney General in charge of OCTF, or one of his assistant deputies, may conduct investigative hearings, compel the production of documents and other evidence, apply

---

<sup>50</sup>Prior to taking charge of OCTF, from March 1999 to September 2002, I served as Assistant Deputy Attorney General in the OAG's Criminal Division. Prior to my employment with the OAG, I was employed by the New York City School Construction Authority, Inspector General's Office, as First Assistant Inspector General and Counsel to the Inspector General. I began my career as a prosecutor for the Manhattan District Attorney's Office where I worked as a trial assistant to the Career Criminal Prosecutions Bureau, as Senior Investigative Counsel in the Rackets Bureau, and as Deputy Chief of the Frauds Bureau. Prior to moving to New York, I was employed by the North Carolina Attorney General's Office. I earned my juris doctorate from the University of North Carolina School of Law in 1977, and am admitted to practice in the States of New York and North Carolina.

for search warrants, and, with the consent of the Governor and the appropriate district attorney, appear before grand juries, conduct criminal and civil actions, and exercise the same powers as the local district attorney.

Court-Authorized Wiretaps Are Essential To OCTF

5. Article 700 of New York's Criminal Procedure Law governs court-authorized eavesdropping in New York by state and local prosecutors and complies with the Federal eavesdropping standards set forth in Title III of the Omnibus Crime Control and Safe Streets Act, 18 U.S.C. § 2510 *et seq.* In Article 700, the State Legislature specifically enumerated the serious offenses, such as kidnapping and narcotics trafficking, for which an eavesdropping warrant may be authorized.

6. As the Deputy Attorney General in charge of OCTF, I am authorized by statute and the Attorney General to determine when it is necessary and appropriate to seek court authorization to use wiretaps and pen registers and to personally apply to the appropriate court for an eavesdropping warrant. Wiretap warrants are issued for up to thirty days, and a new application is required to obtain an extension warrant for each additional thirty days. If a carrier delays provisioning and thus prevents the interception of useful evidence in the initial warrant period, it can be very difficult to obtain an extension beyond the initial warrant period.

7. In the past two years, OCTF has secured court orders for pen registers and/or eavesdropping warrants on more than 440 instruments.

8. One hallmark of any organized group is the need of its members to communicate. This is true of organized criminal enterprises too, whether they be members of a Mafia family, a narcotics trafficking conspiracy, or a terrorist cell. Especially where a criminal organization has a

hierarchical structure, the “street level” offenders too often are the only visible targets for law enforcement. In the narcotics model, for example, only those persons selling small amounts on street corners, within view of the police, are likely to be arrested. Through the use of court-authorized wiretaps, evidence can be gathered against the upper echelon of the organization and criminal responsibility properly can be affixed for all members of the enterprise.

9. OCTF has investigated numerous sophisticated criminal enterprises through the use of court-authorized wiretaps. The evidence obtained through such wiretaps has led to convictions in recent significant prosecutions of organized crime members. OCTF court-authorized wiretaps on wireless phones of Gambino organized crime family associates produced key evidence that led to the RICO conviction of Gambino boss Peter Gotti. *See U.S. v. Gotti*, No. 02-CR-606(FB) (EDNY). Similarly, OCTF taps on the wireless phones of the associates of Joel Cacace, the boss of the Colombo organized crime family, resulted in evidence that led to Cacace’s indictment. *See U.S. v. Cacace*, No. 03-CR-191(SJ) (EDNY).

10. On the non-traditional organized crime front, court-authorized wiretaps have proven critical as well. For example, OCTF’s wiretaps on land lines and wireless phones of individuals associated with the Cali drug cartel resulted in the conviction of more than 450 upper-level drug dealers and the seizure of more than eleven tons of cocaine and more than \$60 million cash.

11. Since the events of September 11, 2001, OCTF has undertaken new types of investigations designed to combat terrorism. Accordingly, OCTF currently is using its wiretap capability and authority to investigate certain types of crimes that commonly are used to finance terrorist activities, including cigarette smuggling, cellular phone fraud, and narcotics money laundering.



Changes In Technology Are Thwarting OCTF

12. A decade ago, most pen register orders and eavesdropping warrants were executed on traditional “land line” telephones. To do this, the carrier identified the copper wire pair and pole location so that a law enforcement technician could attach a device to route call data and/or conversations occurring over the target line to the eavesdropping “plant,” where call data was collected. Monitoring officers then listened to and recorded the target’s conversations. The transmission from pole to plant occurred over a “plain old telephone service” or “POTS” line, the bill for which was part of law enforcement’s cost for the eavesdropping.

13. For electronic surveillance, the advent of packet-mode and IP based communications services eliminates the wires and the telephone pole, and changes the job of the technician from “wire man” to computer specialist. Within minutes of receipt of the court order, warrants for the interception of wireless devices can be implemented by the communications carriers. With just a few computer key strokes, the connection is made directly between law enforcement’s computerized listening stations and the telephone service provider’s computerized switches. These connections occur over expensive, high-speed data lines, leased by OCTF.

14. As a result of the evolution from POTS lines to wireless phones and packet-mode and IP based services, the OAG has spent more than \$4 million in the past three years to upgrade its eavesdropping technology. Despite such investment, we continue to fall behind. For example, each of the major wireless carriers currently offers broadband-based wireless communication services that cannot be tapped, and which can be purchased for only a few hundred dollars.

15. I have no doubt that technologically savvy culprits will continue to utilize the newest, untappable technologies in an effort to thwart electronic surveillance. Wiretap-proof wireless phones and services are available to anyone with a modest amount of funds. While some wireless and VoIP providers offering packet-mode and IP based services have made these services accessible to law enforcement, many of these services remain untappable pursuant to a court ordered wiretap. It is the most technologically savvy criminal groups, those who use untappable services for their communications, for whom we most need to have viable eavesdropping capabilities.

16. The NY OAG has recently experienced the critical importance of the accessibility of VOIP technology to law enforcement's interceptions. Earlier this year, the NY OCTF executed a court-ordered wiretap on a Verizon wireline phone that was being used in furtherance of narcotics related crimes. Just a day or two after the interception was implemented, the target switched service providers, choosing a VOIP service provided by Time Warner Cable and retaining the same phone number. Time Warner Cable cooperated with the New York State police in facilitating the implementation of the court-ordered interception and the wiretap was put into effect. As a result of this wiretap, the OCTF wound up seizing four kilos of cocaine, an extraordinary amount for Central New York, and arrested eight individuals.

Wireless Carriers Appear To Be Making Electronic Eavesdropping A Profit Center

17. Collectively, the phone companies charge OCTF between \$400,000 and \$500,000 annually for the cost of implementing interception court orders. This charge is over and above the monthly connection charges (\$110 for in-state and \$200 for out-of-state) for maintaining high speed data lines connecting the phone companies' facilities to OCTF's equipment.

18. In the past few years, the fees charged to law enforcement by telephone service providers for implementing lawful pen register and wiretap warrants have skyrocketed, to the point that many prosecutor's offices across New York State simply do not have the funds to pay for this crucial investigative tool. The increased costs associated with replacing POTS lines with leased, high speed data lines are only a small part of the overall increase. Over and above those line costs, each telephone service provider assesses its own "provisioning fees." These fees are needlessly excessive as only minimal effort is required on behalf of a wireless carrier to provision an intercept, which is achieved entirely through electronic coding.

19. Set forth below is a description of the provisioning fees charged to OCTF by the major wireless carriers:

a. Nextel charges OCTF \$1,500 per target number to set up an intercept, plus a \$250 monthly service fee for the duration of the intercept. If the target subscribes to Nextel's PTT service (Direct Connect<sup>SM</sup>), an additional \$1,500 setup fee plus \$250 monthly service fee is imposed;

b. Sprint PCS charges OCTF \$250 per "market area" as a setup fee (New York is one market area), plus \$25 per day. When OCTF questioned Sprint about the basis of its provisioning fee amount, the response given was that it was comparable to the fee charged by other carriers;

c. T-Mobile applies yet another formula. Connections to ten or more switches are typically needed to implement a pen register or wiretap warrant on a T-Mobile wireless phone. T-Mobile charges OCTF \$250 per switch for each pen register and/or wiretap for the initial 30 days (up to a maximum of \$2,500) for each target phone number, plus a \$100 "bridging fee" per target phone number. Extensions are assessed a \$50 per switch fee (up to a maximum of \$500), plus the bridging fee, per target number. (Additionally, Voice mailbox "cloning" costs \$150 for each 90-day period, per target number.) In practical terms, these fees equate to a charge of \$2,600 per wireless phone tap for the initial 30 days, and \$600 per wireless phone for each additional 30 day extension;

d. Cingular Wireless charges a flat \$600 processing fee per target;

e. AT&T Wireless charges OCTF double for most intercepts. Separate New York criminal procedure statutes govern pen registers and wiretaps. Accordingly, OCTF typically must apply for simultaneous authorizations and the court issues a separate eavesdropping warrant and pen register order. Even though OCTF serves AT&T Wireless with both the warrant and order together

and no extra effort is required, AT&T Wireless insists on charging OCTF separate fees of \$2,200 each for provisioning the pen register and the warrant, for a total of \$4,400. If the pen register and wiretap were combined in a single court order, AT&T Wireless would charge a single fee. At one time, Nextel maintained a similar double billing policy, but changed it when questioned by OCTF, and acknowledged that there was no justification for billing additional amounts for wiretap warrants and pen register orders when they are served together; and

f. For each target line to be intercepted, Verizon Wireless charges OCTF a \$50 “administrative fee” plus a \$25 per switch set-up fee, in addition to a \$800 per switch “service and maintenance” fee (or a \$2,000 monthly service and maintenance fee for three or more switches). Monthly extensions for each intercept cost an amount similar to the initial setup, even though there is no significant effort or cost incurred by Verizon for not de-provisioning the intercept.

20. The intercept provisioning charges of wireline carriers are much less than for wireless carriers, and are comparable to fees such carriers charge for installation and maintenance of single line business service.

21. When challenged for what OCTF has come to view as exorbitant charges for implementing lawful pen register orders and eavesdropping warrants, the phone companies have proffered various justifications for their fees. One company at first claimed money was owed for time spent by its legal staff reviewing the warrant, and even went so far as to request that copies of the eavesdropping application and supporting affidavits, upon which the issuing judge found probable cause, be furnished to it for inspection and review. No such fee was required in the days of POTS lines and the orders and warrants are the same now as they were then. Moreover, applications and supporting affidavits are sealed as a matter of law and have never been available for telephone company review. When OCTF explained this, there was no diminution in the eavesdropping fee. Instead, the company claimed to OCTF that the fee schedule represented an amortization of its costs for CALEA compliant switches.

---

J. Christopher Prather

The foregoing affidavit was signed before me by J. Christopher Prather, known by me to be the person identified above, on this 8<sup>th</sup> day of November, 2004.

---

Keith H. Gordon  
Notary Public